

DOCKET FILE COPY ORIGINAL

RECEIVED

JAN 26 1993

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
)
Inquiry into Encryption Technology) PP Docket No. 92-234
For Satellite Cable Programming)

To the Commission:

COMMENTS OF TITAN SATELLITE SYSTEMS CORPORATION

TITAN SATELLITE SYSTEMS CORPORATION
3033 Science Park Road
San Diego, CA 92121
619/552-9797

January 26, 1993

No. of Copies rec'd
List A B C D E

0+8

No. of Copies rec'd
List A B C D E

RECEIVED

JAN 26 1993

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Table of Contents

Comments of Titan Satellite Systems Corporation in the FCC Inquiry into Encryption Technology for Satellite Cable Programming

I.	Introduction	1
II.	Benefits of Competition	2
III.	Additional Information on the Linkabit Smart Card System.	5
IV.	Response to Comments by Home Box Office	10
V.	Response to Comments by General Instrument	13
VI.	Conclusions	18

Appendix 1 - Abstracts of United States Patents

Appendix 2- Letter from RSA Laboratories

RECEIVED

JAN 26 1993

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
) PP Docket No. 92-234
Inquiry into Encryption Technology)
For Satellite Cable Programming)

To the Commission:

COMMENTS OF TITAN SATELLITE SYSTEMS CORPORATION

I. INTRODUCTION

The Commission has received significant information in connection with its inquiry into encryption technology for satellite/cable programming. Central to this review of the Home Satellite Dish (HSD) market is the Commission's expressed belief in the value of competition. The Commission writes (NOI, page 2, paragraph 2), "We continue to believe that competition in the home satellite dish market place is likely to benefit consumers by providing an increasing range of choices both in program sources and in user-friendly reception equipment with sophisticated features and by holding down the prices of these goods and services." The initial responses to this inquiry take two distinct views of this opinion.

The first category of responses strongly endorses the Commission's view of competition in encryption technology. Organizations filing comments supportive of competition include PrimeTime 24, Scientific-Atlanta, DirecTV, News Datacom and the Motion Picture Association of America (MPAA). As indicated in its initial response in this inquiry, Titan Satellite Systems Corporation endorses the Commission view on the benefits of competition and similarly endorses many of the statements and holdings presented by PrimeTime 24, Scientific-Atlanta, DirecTV, News Datacom and the MPAA.

The second category of submissions in this inquiry express the views of companies strongly opposed to competition in the C-band descrambler market. Companies supporting this viewpoint are General Instrument Corporation and Home Box Office, a division of Time Warner L.P. This is, of course, not particularly surprising since General Instrument holds a monopoly on the supply and manufacture of today's descramblers, and HBO has historically received annual royalty payments in the millions of dollars from General Instrument. (It is widely accepted throughout the HSD industry that this practice continues today). Their combined opposition to competition seeks once again to have the Commission reject normal regulatory practice for monopolies, and, thereby, tacitly endorse and permit the continuation of monopolistic practices that have hurt the HSD market for more than seven years. Their effort is clearly designed to have the Commission sanction market and commercial privileges and advantages that neither organization could obtain in a normal, rational and competitive market.

Titan Satellite Systems Corporation strongly supports intra-VCII competition and firmly believes such competition will result in lower-cost, higher-security HSD systems for consumers and will also provide the basis from which the C-band market can expand. A more healthy C-band market, whether analog, digital or hybrid in nature, should emerge – with effective descrambler competition -- and develop into a technology that can provide on-going meaningful competition to the cable television industry, the yet-to-be-launched, high-powered Direct Broadcast Satellite (DBS) services, and other means of television transmission and distribution.

In its Reply Comments, Titan Satellite Systems Corporation provides supplemental information in support of the filings submitted endorsing intra-VCII competition, additional information on the nature of the operations of the Linkabit Smart Card System (LSCS™) technology that is being manufactured and specific responses to the highly unusual and frequently erroneous and misleading claims and contentions offered by General Instrument and HBO as rationales for opposing intra-VCII competition.

II. BENEFITS OF COMPETITION

Titan Satellite Systems Corporation, in its initial filing, provided the Commission significant documentation regarding the benefits that intra-VCII descrambler competition would provide both consumers and those businesses that serve today's HSD market. Among the immediate benefits cited by Titan Satellite Systems Corporation are:

- Lower wholesaler prices for descramblers
- Lower consumer prices for HSD systems

- Increased security
- Greater responsiveness to market needs for security enhancements
- Market expansion in hardware and programming sales
- Increased investments in hardware research and development
- Increased consumer participation in existing conversion programs
- Enhanced service

As it prepared its initial comments for the Commission, Titan Satellite Systems Corporation executives came to the conclusion that it was unlikely that its supporters would risk filing public comments in this proceeding. Original equipment manufacturers and distributors who have signed purchase agreements with us have requested that no public disclosure be made. As documented in our initial filing, programmers are now operating under a General Instrument threat of either lawsuits or termination of service and support should they decide to work with Titan Satellite Systems Corporation, and, therefore, were unlikely to file public documents with the Commission supporting competition.

It is therefore particularly noteworthy that of the eleven organizations which submitted comments in this proceeding and are currently active in the HSD market place today, six filed comments in support of intra-VCII descrambler competition. Furthermore, these groups and their comments are noteworthy because of the nature of their business and their current or future role in the HSD marketplace. The organizations in addition to Titan Satellite Systems Corp. are:

- *PrimeTime 24*; a major program distributor, rebroadcasting network television programming, which established its principal business and derives the majority of its revenues from serving the HSD market;
- *The Motion Picture Association of America*, which represents the major studios that provide the majority of video product distributed by cable/satellite programmers, and, which played a principal role in forcing General Instrument to respond to piracy with an investigative program;
- *Scientific-Atlanta*, a large supplier of equipment to the cable industry, a distributor of VideoCipher commercial descramblers and a leader in the cable industry's move to digital transmission;
- *DirecTV*, a new DBS service that will compete with Titan Satellite Systems Corporation and other C-band business entities; and,
- *News Datacom*, a manufacturer of smart card systems and provider of encryption and conditional access systems, which also is a competitor of Titan Satellite System Corporation.

We believe that a number of conclusions reached independently by these organizations provide strong evidence that competition in the VCII descrambler market will benefit consumers and others in these areas:

a. Lower prices for consumers.

PrimeTime 24 writes, "It is the firm belief of PrimeTime 24 that competition in the supply of encryption equipment and technology will be extremely helpful to the industry by not only ensuring the availability of the lower equipment costs ..."

News Datacom's comments to the Commission include the following, "The NDC approach will facilitate competition among programmers, IRD manufacturer's and access control providers, driving down costs to consumers."

Scientific-Atlanta states, "As in any marketplace, competition works to lower prices and increase the features offered to consumers. Competition in the satellite encryption market would have the same effect on modules and IRDs."

The MPAA similarly writes that "the MPAA member companies strongly endorse the idea of competition in the market place as the best means of producing the most secure technology at the lowest cost to consumers."

b. Incentives for security enhancements and timely consumer upgrades.

PrimeTime 24 writes, "Clashes with programming pirates will be repeated. When they are, competitive supply of encryption equipment will ensure the fastest and most complete response, even to the detriment of then current inventories of compromised equipment.¹ Without real competition in the industry, solutions may be slow in coming or incomplete, to the continued detriment of the industry and HSD consumers."

Scientific-Atlanta similarly notes, "Competition would also give programmers more options in dealing with suppliers regarding an upgrade by forcing manufacturers to compete on the price and availability of "smart cards."

c. Module supply.

PrimeTime 24 writes that it "shares the concern voiced by many in the industry that GIC will not be able to adequately address the immediate demand for VCII Plus units for many months, if not years."

¹ As General Instrument was beginning to ship VCII Plus units in the latter part of 1989, it continued to supply thousands of easily piratable VCII units until inventory was depleted. These very units are now being "turned off," and their owners must purchase a new VCRS or VCII Plus unit to continue to view satellite TV programming.

d. *The current trend in the digital migration will perpetuate today's monopoly.*

Scientific-Atlanta offers important statements regarding the transition to a digital world that will require IRDs with both digital and analog descramblers. It writes, "Because the new decoder must be able to decrypt the existing analog signals, and because the current DBS center will likely service the new digital/analog subscribers, the current de facto monopoly maintained by VCII will continue into the digital world any manufacturer wishing to serve this market will be at a significant disadvantage, if they are able to compete at all, to GIC.

III. ADDITIONAL INFORMATION ON THE LINKABIT SMART CARD SYSTEM

A number of technical issues regarding the installation and operation of the Linkabit Smart Card System require clarification in light of comments made in the initial filings in this NOI, particularly regarding comments from General Instrument and HBO. We must note that while it is certainly possible to refute comments made by these companies regarding DBS Center issues, we will refrain as we do not seek Commission-sanctioned access to the General Instrument Center, as we are nearing completion of our own authorization center.

Titan's Ownership of Key VideoCipher Patents:

In its response to the NOI, General Instrument raises several issues regarding the technology used by Titan Satellite Systems Corporation's Linkabit Smart Card System descrambler modules. General Instrument tries to cast the LSCS system as old VCII-based technology in the hopes that the Commission will conclude that the LSCS system will be immediately pirated as was the VCII system. At the same time, General Instrument tries to convince the Commission that its newest generation of VCII descrambler, the VCRS descrambler, is based upon new proprietary encryption technology that is a radical departure from VCII and therefore unavailable to its competitors. An examination of the technologies used in the LSCS, VCII Plus and VCRS descramblers does not support General Instrument's position.

As shipped to the end-user, each VCII Plus and VCRS descrambler module consists of a descrambler circuit card assembly enclosed in a sealed plastic housing. Along with various labels showing regulatory compliance, General Instrument imprints a legal notice regarding the patents, copyrights, trademarks and licenses used during the manufacture of the VCII Plus and VCRS descramblers. Line b of the notice cites the patents covering the VCII Plus and VCRS descramblers. It reads: "U.S. Patent Nos. 4,608,456; 4,613,901, 4,634,808; 4,712,238; 4,792,973; 4,864,615; 4,933,898 and patents pending." Of the seven U.S. Patents cited, the Titan

Corporation as the successor corporation to M/A-COM Linkabit, Inc. and M/A-COM Government Systems, Inc. is the co-assignee of the first five. The remaining two patents are assigned to General Instrument and relate to minor improvements to the VCII descrambler resulting from the completion by General Instrument of the VCII Plus system design substantially performed by M/A-COM Linkabit prior to its acquisition by General Instrument; accordingly, Titan Satellite Systems Corporation is extremely familiar with the VCII Plus design and the changes from VCII to VCII Plus. The intellectual property, if any, covered by the "and patents pending" portion of the notice remains unknown at this time, however, given the breadth of the coverage of the five core VideoCipher patents it is unlikely to be significant. The abstract of each of the U.S. Patents cited above is included for convenience in Appendix 1.

Several conclusions can be drawn by the consideration of the facts presented above. First, the Titan Corporation owns the fundamental intellectual property necessary to develop a security product that is competitive with General Instrument's VCII Plus and VCRS descramblers. Second, except for some details relating to the physical security of the cryptographic processor and the addition of a smart card slot in the VCRS, the VCRS and VCII Plus descramblers, no matter what General Instrument would have us believe, are essentially VCII descramblers. Third, if General Instrument can make minor design implementation changes to its descrambler and field a product with significantly improved security, it stands to reason that with the intellectual property cited above and the proper engineering staff, the Titan Corporation is capable of doing the same.

Finally, General Instrument implies that the Titan Corporation does not have the "inventive talent" required to design and field a competitive security product. The facts are that the Titan Corporation currently has in its employ, two of the inventors named in four of the core patents cited above. As disclosed in its response to the NOI, Titan Satellite Systems Corporation has incorporated many sophisticated cryptographic concepts into the LSCS system design that will allow a flexible yet cost effective response to any pirate attack.

System Security, Compatibility and Control Channel Transmission:

In its response to the NOI, HBO raises several issues relating to system security, compatibility and control channel transmission bandwidth that are important concerns to programmers when considering whether or not to authorize a competitive encryption system. Titan Satellite Systems Corporation takes very seriously HBO's concerns regarding the piracy of its programming. Unfortunately, some of HBO's statements relating to system compatibility and security seem to be based upon folklore rather than a sound understanding of the VCII, VCII Plus and VCRS encryption technologies. An examination of the facts will clear up the confusion.

The question of whether or not system security will be degraded or enhanced with the addition of competitive descrambling equipment is critical. Titan Satellite Systems Corporation has given this issue very serious consideration in the design of the LSCS system. Let us first examine the question of whether or not VideoCipher system security would be degraded by the presence of a competitive yet compatible security system.

The designs of the VideoCipher and LSCS cryptosystems are based upon a hierarchy of cryptographic keys. At the highest cryptographic level the keys change infrequently (e.g. once a month) but at the lowest cryptographic level the keys change very frequently, in this case 7.5 times per second. The LSCS maintains compatibility with the VideoCipher system at the lowest level while being divergent at the intermediate and higher levels. In general, cryptosystems can be compatible at the lowest levels without impacting system-wide security. Of course, in order to achieve the desired level of system-wide security performance, each of the separate compatible cryptosystems must be properly designed both in terms of the security level of the system as initially fielded, and in terms of its ability to respond cost effectively to continuous pirate attack. The design of the LSCS cryptosystem succeeds in achieving these goals -- that is, the LSCS cryptosystem design achieves an exceptionally high level of security with cost effective strategies for dealing with continued attempts by the pirate to breach the system while maintaining cryptographic separation from the VideoCipher system so that a breach of either system will have no effect on the other.

Titan Satellite Systems Corporation has submitted its cryptosystem to RSA Laboratories for review. RSA Laboratories is an independent, nationally recognized cryptosystem analysis firm. RSA Laboratories has found the LSCS cryptosystem to be exceptionally well designed and implemented, incorporating advanced cryptographic techniques and physical security strategies that will keep the LSCS system ahead of the pirate for years to come. We have asked RSA Laboratories to analyze the effect that the LSCS cryptosystem would have on the security of the VideoCipher II Plus (including VCRS) system. Dr. Burton S. Kaliski Jr. of RSA Laboratories writes (see Appendix 2), in response to a specific request by Titan Satellite Systems Corporation to address this issue:

"The coexistence of multiple security systems with common cryptographic keys raises important concerns. The security of any system, it is often said, is only as high as the lowest fence. A pirate will attack whichever system is weakest.

Two provisions are essential. Fence "height" must be measurable, to some degree; a security provider with a low fence should not be permitted to interoperate. And fence "crossings" must be detectable. If a pirate does attack a system, it should be possible to determine which system the pirate attacked.

The Linkabit Smart Card System and VideoCipher II (and II Plus) interoperate only at the channel [program] encryption level, not at the conditional access/key management levels.

It is generally not practical to attack a system at the channel encryption level because the channel encryption key changes so frequently. An attack on either system will therefore, most likely, involve not the interoperable parts, but the different parts. Pirated descramblers will contain software and keys implementing one system or the other. It follows that fence crossings can be detected.

Coexistence of the Linkabit Smart Card System and General Instrument's VideoCipher II Plus system therefore does not necessarily weaken security. Indeed, it is possible that the introduction of new systems, properly reviewed, will strengthen security overall."

As Dr. Kaliski points out, the introduction of the LSCS system as a competitive yet compatible security system has the potential to actually increase system-wide security performance through true competition among security system providers.

The other security related issue has to do with HBO's insinuation that the LSCS system is based upon hopelessly compromised VCII-like technology simply because it uses the horizontal blanking interval (HBI) to transmit its authorization and control channel. While it is certainly true that the VCII consumer and commercial descramblers are hopelessly compromised due to the inadequacy of physical security implementation of both descrambler's cryptographic processor and the large quantity of these descramblers sold by General Instrument from 1986 to 1990 (estimates are that 1.8 million VCII consumer descramblers were sold), this has no bearing upon the security of the LSCS system. That is, the VCII Plus and VCRS systems are not more secure because they use the vertical blanking interval (VBI) to transmit their authorization channel nor is the LSCS system less secure because it uses the HBI for this purpose.

Furthermore, HBO implies the LSCS system uses the VCII consumer and/or commercial authorization channel for its authorization channel such that the introduction of the LSCS system as a competitive security system would result in a return to the days of rampant VCII piracy. This statement is not only untrue but irresponsible. HBO executives and engineers have been fully and extensively briefed by Titan Satellite Systems Corporation in regard to the technical approach taken in the design of the LSCS system. HBO knows full well that the transmission of the LSCS system authorization channel does not involve a security risk since it does not involve the maintenance or reintroduction of any VCII cryptographic messages or any other messages that can possibly be of use to the pirate. In fact, an HBO Director of Engineering, upon reviewing the LSCS system design, reported this fact to the appropriate HBO executives. In addition, when asked to recommend the best option for the transmission of the LSCS system authorization channel (i.e., the HBI or the VBI) the same individual recommended the HBI as the best option since the HBI was being vacated. Again, this issue is critical and has been reviewed by RSA Laboratories. Regarding this issue, in the same letter mentioned previously, Dr. Kaliski writes:

"HBI transmission of a digital control channel is intrinsically no more or less secure than VBI transmission. Cryptographic security depends on how the bits are protected, not on special analog characteristics of the interval. Whether the control channel is in the HBI or VBI has no impact on the difficulty of obtaining keys.

The fact that the VideoCipher II control channel is in the HBI and VideoCipher II descramblers are easily "pirated" may suggest to some that the HBI is easily pirated. But the VideoCipher II piracy has nothing to do with HBI or VBI transmission. It has everything to do with weaknesses in the descrambler's physical security."

VCII piracy will not end until all VCII authorizations are completely eliminated. In regard to HBO's plan to upgrade their VCII commercial descramblers and eventually shut down the VCII commercial authorization channel in 1993, Titan Satellite Systems Corporation applauds this and in fact will offer programmers a cost competitive LSCS commercial descrambler in order to help hasten the upgrade. It has been estimated that the cost of such an upgrade to the HSD industry could reach \$50-60 million. However, HBO's statement that "With the advent of VCRS, prospects are bright that home satellite piracy can be significantly curtailed." remains to be seen. The shut-off of the VCII consumer authorization channel required by the recent upgrade program was supposed to eliminate piracy, but the pirates have turned to the VCII commercial authorization channel and piracy of programming is still rampant and will continue as long as there is no economical means of repairing breaches in the security system. The prospect for eliminating piracy of the VideoCipher system is not bright as long as General Instrument has no economic incentive to do so.

Notwithstanding the above, additionally there are in excess of 500,000 VCII Plus consumer descramblers in the field that cannot accept a smart card. This means that when the VCII Plus system is breached General Instrument will have no economically practical means to repair the security breach. Unless Titan Satellite Systems Corporation is allowed the means to compete effectively in this market, there will be no business incentive for General Instrument to eliminate piracy.

The question of system compatibility is another critical issue when considering a competitive security system. The LSCS system is quite unique in this regard. The LSCS system is the only competitive system that protects the huge investment in scrambling equipment made by programmers as well as the manufacturers of VideoCipher compatible consumer and commercial IRDs. The LSCS consumer and commercial descramblers use the industry-standard IRD electrical and user interfaces popularized by the VideoCipher II system. Thus the IRD manufacturer can protect his investment in tooling and software. The HSD owner is able to enjoy HSD satellite service by purchasing an IRD equipped with a low-cost LSCS descrambler module, or can upgrade his VCII module to a LSCS module while enjoying a compatible but improved user interface.

Finally, HBO raises the issue of authorization channel access for a competitive security system and talks about the burden placed upon it if the Commission required such access. Again, there is confusion as to the operation of the VideoCipher system. That portion of the HBI that is presently used for authorization messages, and is being vacated as a result of the elimination of consumer and ultimately commercial VCII control information is a very specialized "digital highway" that is only suited to the transmission of authorization, control and specialized data messages called HDLC message packets. It is not suitable for the transmission of audio data and other general purpose data, and in fact the uplink scrambler has special facilities for those purposes.

As described in our initial filing, the LSCS technology provides a seamless interface with today's currently used technology that is transparent to consumers and simple for programmers to implement. Our system does not impinge on the General Instrument operating system, transmissions or cryptography.

IV. RESPONSE TO COMMENTS BY HOME BOX OFFICE

The comments of Home Box Office fall into two general categories – technical and "posturing." The previous section of our Reply Comments provides the technical information about the LSCS technology and eliminates concerns raised by HBO, particularly regarding the HBI, VBI, bandwidth and the like. This same information has been provided to HBO as often as possible prior to its filing in this inquiry.

In the area of market posturing, we are concerned that a number of HBO positions are contradictory and frequently misleading.

For example, HBO writes (at page 13):

"From HBO's perspective, it is inconceivable that a programmer who has lost millions of dollars in revenue from pirated VCII equipment would utilize a product that incorporates HBI transmission of a technology based upon VCII. Therefore, HBI would only consider an alternative encryption technology without any links to, and which does not use, the compromised VCII or VCII-like technology transmitted in the HBI."

HBO, seemingly by design, does not inform the Commission that the VCRS technology which it presently endorses is based on VCII technology. In fact, on page 7 of its submission HBO writes, "By April 1990, HBO had begun using a more secure version of VCII, called VCII Plus". In fact, the Commission really need look no further than the information imbedded in the

plastic housing which encloses the VCRS module, which itemizes the VCII patents that are incorporated in the VCRS technology.

Titan Satellite Systems Corporation continues to seek a business relationship with HBO and would prefer not to publicly rebut and refute HBO's initial comments that are of a posturing nature in the areas of competition, the transition to digital systems, security, price and consumer confusion. However, the misleading nature of many of HBO's comments require our response.

a. Competition, the digital migration and retail price.

HBO writes at page 3 of its submissions that "rather than focus on competition within the C-band analog system, the Commission, in HBO's view should recognize the more significant inter-system competition that will soon be a reality in the United States." On page 4, this leading programmer writes, "The programming offered by these competing services (DBS and C-band) in all likelihood will be similar; the distinguishing factor will be the features and cost of the hardware and programming available from each source. If the C-band HSD industry is to meet the competition, HBO believes that there will be a dramatic decrease in C-band equipment prices driven naturally by increased competitive pressures." It further states at page 5 that "... if C-band analog equipment prices remain sufficiently higher than digital equipment prices, there will be business incentives to complete the transition to more secure and less expensive digital hardware."

We also find it contradictory at best when HBO argues at page 12 of its filing that competition will come within a particular HSD market where competitive hardware technology is widely licensed and when alternative technology competes with diverse encryption systems. Since broad licensing has been rejected by General Instrument, and HBO for that matter based on its comments in this proceeding, will C-band competition occur? More importantly, if licensing is an appropriate pro-competitive factor why is there a problem with co-ownership of key underlying patents that allow manufacture and sale of equipment so compatible as to be transparent to consumers?

In essence, HBO is saying to the Commission that monopoly practices in C-band should be allowed to continue in the descrambler segment and that competition in this segment is unnecessary because DBS is coming. One must ask why competition is acceptable in DBS encryption but not in C-band encryption. As Titan Satellite Systems Corporation reported in its initial filing with the Commission, the Company is engaged in development programs that will drive down the cost of descramblers beyond the 30 percent price reduction achieved with its initial product. This type of cost-reduction will ultimately create the opportunity for C-band equipment manufacturers to offer retail prices competitive with those announced by DBS proponents.

Two other points are troublesome in HBO's comments on competition. One is the suggestion that programming will be similar. That would seem to be premised on cable programmers willingly and readily complying with the recent congressional legislation mandating access to cable programming for DBS and other alternative distribution systems. The Commission and the HSD and DBS industries can hardly take this as an article of faith from HBO since its parent company, Time Warner Entertainment Company, L.P., was the first to initiate court action to block implementation of the cable act.

Secondly, the Commission and HSD industry cannot accept at this time the argument that lower priced DBS consumer equipment will force reductions in C-band equipment prices. General Instrument certainly has no experience in lowering prices in the HSD market. Its much touted alliance with HBO, TCI and AT&T is solely focused on DBS. How can the HSD industry truly believe General Instrument would lower its C-band prices, when as HBO has so carefully noted, high C-band prices will expedite a forced migration to DBS and hasten the demise of C-band television viewing? As we noted in our initial filing, only one element remains as a barrier to lower prices for C-band receivers and that is the descrambler cost. If General Instrument and its royalty partner can block competition and maintain their abusive VideoCipher module monopoly, they can continue to enjoy unseemly profits from the C-band module, keep C-band modules prices high, perhaps even higher than today's level if historical trends apply, and thus force consumers to DBS, once again under a proprietary monopoly and on their exclusive terms.

This concern is heightened by General Instrument's announcement last week of its planned introduction of a digital/analog DigiCipher receiver with both a VCRS descrambler and an NTSC all-digital descrambler for DBS services, both based on General Instrument's proprietary technology. In point of fact, on page 24 of its filing in response to this NOI. HBO writes, "Initially, HBO is requiring its digital compression vendors to supply IRD's with both digital and analog compatibility."

Scientific-Atlanta accurately outlined for the Commission the impact of such an extension of the General Instrument monopoly. It wrote: "It appears that TVRO subscribers will be required to purchase a new satellite receiver and decoder module ... Because the new decoder must be able to decrypt the existing analog signals, and because the current DBS center will likely service the new digital/analog subscribers, the current de facto monopoly maintained by VCII will continue into the digital world." Scientific-Atlanta notes that in this new digital world under a General Instrument de facto standard monopoly, manufacturers will be required to purchase at least an analog VCRS module from General Instrument and in all probability a DigiCipher digital module. Scientific-Atlanta concludes, "In either case any manufacturer wishing to serve this market will be at a significant disadvantage, if they are able to compete at all, to GIC."

b. Consumer confusion.

HBO seems to raise an objection to competitive, alternative systems stating they must have virtually identical features lest consumers become confused. This view of competition -- and a concomitant denigration of U.S. consumers -- is at best unusual. If HBO truly believes this to be the case in a competitive world, then surely it must believe that TVRO consumers also are addled when HBO and Showtime offer different programming and even when similar, offer it on different schedules.

c. Second source manufacturing.

Again in the area of competition, we find it distressing at page 11 to find that HBO attempts to mislead the commission regarding the so-called second source manufacturer. Channel Master simply is not manufacturing VCRS modules; it purchases complete modules from General Instrument, loads "seeds", does a quality check and forwards the modules through the HSD distribution network.

V. RESPONSE TO COMMENTS BY GENERAL INSTRUMENT

As with its ally, HBO, the initial comments by General Instrument are to challenge the technical features of the LSCS technology, followed by a series of strained comments attempting to justify its monopoly and its efforts to block market entry by Titan Satellite Systems Corporation. We respond to the second of these categories here:

a. The smart card.

At footnote 11, General Instrument offers a rationale for the industry to accept only its approach to smart cards, stating it is imprudent to issue smart cards prior to a system compromise and then to do so only after the nature of the compromise was fully analyzed. This type of contention lays the foundation for a repeat of the VideoCipher II fiasco in which it took General Instrument nearly six years to develop a "solution".

It has been suggested in industry publications and is generally believed in the HSD industry that General Instrument's upgrade contracts with programmers contain language that narrowly defines a compromise, requires that a least 75 percent of programmers using the VCRS technology agree to an upgrade (a percentage requirement that literally means HBO, Showtime and perhaps Netlink as occurred with the VCII recall program, rendering all other programmers

and their security needs immaterial), and a time period of substantially more than one year to initiate an upgrade.

The industry simply cannot afford this situation, setting the stage whereby General Instrument through its monopoly powers and its market power can be the sole determiner of when security is broken and how it will be repaired.

b. The "second source" manufacturer and the control of module supply.

General Instrument joins HBO in attempting to portray once again that a true second source manufacturer of VC modules exists. This is simply not the case. Channel Master is merely a distributor of modules for General Instrument. To continue this manufacturing claim must be construed as either arrogance or a deliberate effort to mislead the Commission.

General Instrument contends that Channel Master has held, at times, 60 percent market share. It does not state how much of Channel Master's inventory of General Instrument-manufactured modules were "sold back" to General Instrument for use in its IRD line or for sale again to other manufacturers. This "arrangement" was in place to assist the two companies in inventory management, and is obviously not a typical situation one would find in a true, arm-length competitive relationship.

General Instrument further asserts that there is no empirical evidence of its control over module supply. General Instrument could certainly end any controversy by providing the Commission all records related to its relationship with Channel Master and its supply of modules to Channel Master.

Nevertheless, there is empirical evidence that clearly shows that there is no difference between the design and layout of the descrambler board between General Instrument's module and the so-called Channel Master module. The parts on the descrambler board from each company are identical, the availability and advance-order requirements are the same. And the price is essentially the same, although Channel Master is slightly lower priced at lower volumes, while General Instrument is slightly lower priced at larger volumes. Another example of empirical evidence of General Instrument's control over the module supply relates to the Modern on Module (MOM) descrambler. Although requested by many IRD manufacturers, General Instrument refused to supply a lower priced version of the module without the modem and "forced" module purchasers to buy the MOM version only. When Channel Master's non-MOM module supply was depleted it followed suit and also only offers the MOM version. Certainly this would not be the case in a truly competitive environment.

With due respect to Channel Master, the evidence is also clear that there is no competition based on price, with Channel Master stating in its filing in this inquiry that it sees no advantage in price competition with General Instrument. In other words, if General Instrument

can “get away with it, why shouldn’t we.” There can be no stronger indicator existing in the public domain today of the lack of competition than this.

The industry is now closely watching reports of major quality problems in the VCRS module (Satellite Business News, January 13, 1993) and will have yet another opportunity to assess whether Channel Master is a true second source manufacturer. If it is, will it correct the quality problem with an independently-derived solution, or will it wait for General Instrument to correct the problem? Will it continue to supply General Instrument-manufactured descramblers to its customers despite some reports from licensed manufacturers and distributors of failure rates well in excess of 15 percent? The answer to these two rhetorical questions is “no”, and will be yet another proof of the second-source manufacturer charade.

c. *The “innovation” claim.*

General Instrument at page 9 of its comments suggests that competition, either via second sourcing or exercise of legal rights through co-ownership of patents as is the case with Titan Satellite Systems Corporation, may result in “reduced product variety and stifled innovation.” This claim seems to rest on prior General Instrument arguments against standardization and seems to follow a thought that General Instrument is the only source of product variety and innovation and would not be willing to invest in innovation if the results become widely available to competitors. This certainly is the response of a monopoly. However, within the HSD industry there is certainly strong evidence to the contrary, evidenced by the wide variety in integrated receiver/descrambler and ancillary equipment, offering a full range of features at varying price levels.

It is in fact the ever-present role of General Instrument as a monopoly and sole supplier of modules that has threatened product variety and innovation in IRDs in the past in at least three key ways:

First, an onerous condition of a manufacturer’s license with General Instrument requires the submission of all new receivers to General Instrument for testing and certification months prior to product introduction. Thus General Instrument has been able to see and analyze the product variety and innovations developed by other manufacturers and, at its will, initiate parallel development to compete with competitor’s development of innovative designs, features, and efficiencies that should have been solely the fruits of the licensees investment in research and development.

Secondly, the non-stop escalation in module prices -- absent any significant improvement in system security until perhaps, and we must stress perhaps -- the introduction of the VCII Plus/VCRS module -- has eliminated any cost reductions achieved by licensed manufacturers.

The result of General Instrument's pricing strategy has been clearly to stifle manufacturer investment in R&D to provide greater product variety .

Thirdly, General Instrument's continued requirement that IRD manufacturers continue to incorporate the module within its plastic housing, incorporating many redundant parts, and refusing to provide the IRD manufacturers access to information (non-cryptographic data like program name, next program, etc.) contained within the module has not allowed all the user-friendly features that could be offered to be incorporated by other IRD manufacturers. Additionally, the bulky module requires so much room within the IRD, manufacturers cannot develop a more attractive, slim line version of their product.

We can only conclude, with many others in the HSD industry, that the only impediment to product variety and innovation to date has been the General Instrument monopoly.

Competition will provide a solution to this problem.

d. Consumer prices.

General Instrument offers in support of its monopoly a claim that the price of an HSD system has gone down "despite the increased cost of providing security in a market plagued by theft" (page 11).

It is certainly intriguing that any price reductions in the HSD industry have occurred only in the non-encryption segments as the direct result of competition, and that now General Instrument seeks to identify itself so closely with these price reductions yet separate itself from any need for price sensitivity for the descrambler.

e. The recall of VCII commercial descramblers

General Instrument states in its filing that it will initiate this year a recall of the VCII commercial descrambler. HBO confirms this in its submission. What is noticeably lacking in the comments of either organization is a description at a non-technical level of what exactly will transpire.

As is seemingly always the case with General Instrument in this NOI, General Instrument alludes to its VCII commercial recall agenda by stating (page 16):

"In addition, substantial security upgrades will be implemented to programmers' VideoCipher II Plus and RS scrambling systems to further protect critical information resident in such systems."

This reference is, of course, to General Instrument's plan, among other things, to eliminate the programmers' ability to use the HBI, and thus erect a technical barrier to implementation of the LSCS system. In addition to the elimination of HBI messaging insertion

capability, General Instrument intends to make other scrambling system modifications, under the guise of enhanced security, to further erect entry barriers to Titan Satellite Systems Corporation. These changes, if communicated to Titan Satellite Systems Corporation, would pose no problem to LSCS operation and functionality. Titan Satellite Systems Corporation has been aware for months of this intention and alerted General Instrument to our concern in July of 1992 (see General Instrument's initial filing to this NOI - Attachment of letters from TSSC to General Instrument). General Instrument has elected to interpret those concerns as "building a record."

f. "Violation of Software License and Maintenance Agreements"

On page 26 of its filing, General Instrument writes,

"It would be a violation of the control computer software license to use such software to insert another manufacturer's authorization data stream at a programmer's uplink site."

In its initial filing in response to this NOI, Titan Satellite Systems Corporation provided an opinion from a notable San Diego law firm stating that the function of "appending" a LSCS commercial unit key list utilizing the General Instrument licensed software did not violate the software license agreement. Titan Satellite Systems Corporation has provided that written opinion to all programmers, and subsequently to General Instrument via the initial filing. The programmers merely use the normal "append" function to add LSCS commercial descrambler identities to their database of existing authorizable commercial descramblers. General Instrument's claim is merely their attempt at erecting a non-technical, legal barrier to Titan Satellite Systems Corporation's market entry.

g. "Breaking cleanly with the VCII system."

As indicated above, this section of our Reply Comments references "posturing" statements designed to put a General Instrument "spin" on issues confronted in this inquiry. Perhaps the most interesting "spin" efforts by General Instrument, at page 15, is its claim that "General Instrument determined that it was necessary to break cleanly with the VCII system." Titan Satellite Systems Corporation hopes it has, throughout the technical discussion in this and our initial filing in response to this NOI, been successful at demonstrating that VCII Plus and VCRS are essentially the VCII system, implemented more appropriately. VCII Plus and VCRS certainly are not a clean break from VCII. Even DigiCipher, although an all digital transmission system, uses the same encryption and conditional access system as VCRS according to a General Instrument Engineering executive during a panel discussion at a recent industry trade show; hence, DigiCipher is also not a clean break from VCII. Furthermore, if the desire to break clearly from VCII is genuine, then why hasn't General Instrument abandoned the VideoCipher

name as in VideoCipher II Plus or VideoCipher Renewable Security, or for that matter, DigiCipher?

h. The digital world

Other filers in this proceeding have eloquently stated the concern regarding the extension of the General Instrument proprietary technology and monopoly into the digital world soon to be launched, most notably Scientific-Atlanta.

Again, in Titan Satellite Systems Corporation's initial filing, Titan Satellite Systems Corporation discussed the need for a standard "bridge" between the coming digital video/audio compression technologies and the encryption and conditional access technologies such that multiple systems could be utilized simultaneously, thus avoiding a proprietary, monopolistic situation similar to the one we are now experiencing. On page 42 of its initial response to this NOI, General Instrument writes:

"Another problem raised by universal access is that the costs for particular features must be adopted and paid for by all subscribers, even those who do not want them or will not benefit from them. For example, requiring that all television receivers be digital - compatible would force even those who will not utilize that technology to pay for it."

Presumably, General Instrument believes that it, as a monopolist, should be allowed to decide which features all subscribers must pay for, "even those who do not want them or will not benefit from them." How else can one explain the "forced" purchase by millions of consumers of the little wanted modem installed in each module, or the requirement for consumers to purchase the security warranty contained in each module, at a combined wholesale price for these two features of \$87?

It is apparent to Titan Satellite Systems Corporation from General Instrument's initial filing in response to this NOI that General Instrument wishes to ". . . govern access control to the digital signals . . ." (page 35) just as it GOVERNS access control to the analog signals today.

VI. CONCLUSIONS

Titan Satellite Systems Corporation believes the record of this inquiry shows the clear need for competition in the VideoCipher-based descrambler market, competition that will result in significant benefits to consumers and the HSD industry.

The record to date also shows clearly that General Instrument and others are actively erecting barriers to competition, specifically to block market entry by Titan Satellite Systems

Corporation. General Instrument is acting to block out any programmer access to the horizontal blanking interval of a video signal. It is exerting its market power to threaten programmers who seek to work with Titan Satellite Systems Corporation. And, at least historically, used its market power through the payment of royalties to thwart market entry of a competitive technology.

In seeking furtherance of its de facto standard monopoly, General Instrument seeks a tacit Commission endorsement of this monopoly by asking the Commission to reject any action in this inquiry and thereby permitting General Instrument to continue to act freely and, in our view, abusively, in the continued exercise of unreasonable monopolistic practices and market power.

The Commission in the past has rejected calls for intervening in the HSD market, in particular related to encryption and General Instrument. In doing so, the Commission has eloquently supported the concept of competition, but has concluded that the marketplace is a better determinant of competition than government.

The record in this inquiry shows that the marketplace has been distorted by monopolistic practices which have disserved consumers and severely hindered the potential of satellite television to provide a competitive balance to cable and other television transmission/distribution technologies. The record has also shown via the responses by General Instrument and HBO, coupled with recent industry announcements, that plans to continue this monopolistic situation are well under way.

The Commission faces a dilemma of how to act to support consumers while balancing the protected patent rights of General Instrument and its clearly vested interests.

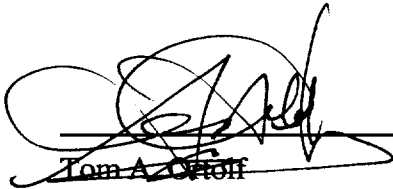
General Instrument has expended considerable energy in its filings to protect its absolute control of the DBS Center, going so far as to state that while the center is a not-for-profit operation, it disputes "any suggestion that GI is trustee for those (programming customers) . . ." General Instrument clearly seeks to continue its ability to "govern" access to programming. While this practice may not be the right market solution, Titan Satellite Systems Corporation does not seek mandated-access to the General Instrument center.

Similarly, we do not seek access to patents, copyrights or intellectual property rights that are not ours.

We seek the opportunity to compete on a level playing field. We do not seek government intervention to obtain market opportunities that would otherwise be available to us in a normal, rational competitive market – the type of market that this Commission is specifically invested to protect.

Respectfully Submitted:

January 26, 1993



Tom A. Orlon

President

Titan Satellite Systems Corporation

3033 Science Park Road

San Diego, CA 92121

619/597-9025

APPENDIX 1

ABSTRACT OF UNITED STATES PATENTS

[54] DIGITAL AUDIO SCRAMBLING SYSTEM WITH ERROR CONDITIONING

[75] Inventors: Woo H. Paik; Jerrold A. Heller, both of San Diego, Calif.; Gordon K. Walker, Boxborough, Mass.

[73] Assignee: M/A-COM Linkabit, Inc., San Diego, Calif.

[21] Appl. No.: 498,824

[22] Filed: May 27, 1983

[51] Int. Cl.⁴ H04M 1/70

[52] U.S. Cl. 179/1.5 S; 179/1.5 R

[58] Field of Search 179/1.5 S, 1.5 R; 371/30, 38; 369/84; 358/310

[56] References Cited

U.S. PATENT DOCUMENTS

3,657,699	4/1972	Rocher et al.	340/146.1
3,731,197	5/1973	Clark	325/32
3,773,977	11/1973	Guanelia	179/1.5
3,789,137	1/1974	Newell	178/6.6
3,819,852	6/1974	Wolf	178/5.6
3,824,332	7/1974	Horowitz	178/5.1
3,824,467	7/1974	French	325/32
3,825,893	7/1974	Bossen et al.	340/146.1
3,893,031	7/1975	Majeau et al.	325/32
3,919,462	11/1975	Hartung et al.	178/5.1
3,921,151	11/1975	Guanelia	340/172.5
3,936,594	2/1976	Schubin et al.	178/5.1
3,970,790	7/1976	Guanelia	179/1.5
4,025,947	5/1977	Michael	358/86
4,171,513	10/1979	Otey et al.	325/32
4,215,366	7/1980	Davidson	358/124
4,266,243	5/1981	Shutterly	358/121
4,275,411	6/1981	Lippel	358/310
4,283,602	8/1981	Adams et al.	179/1.5 R
4,295,223	10/1981	Shutterly	455/72
4,306,305	12/1981	Doi et al.	371/38
4,318,125	3/1982	Shutterly	358/121
4,336,553	6/1982	Den Toonder et al.	358/120
4,353,088	10/1982	Den Toonder et al.	358/120
4,354,201	10/1982	Sechet et al.	358/122
4,364,081	12/1982	Hashimoto et al.	371/30
4,379,205	4/1983	Wyner	179/1.5 R
4,389,671	6/1983	Posner et al.	358/124
4,394,762	7/1983	Nabeshima	371/38
4,410,917	10/1983	Newdell et al.	369/84
4,413,339	11/1983	Riggle et al.	371/38
4,424,532	1/1984	Den Toonder et al.	358/120
4,433,211	2/1984	Calmont et al.	179/1.5 S
4,434,323	2/1984	Levine et al.	178/22.17
4,443,660	4/1984	Delong	178/22.04

FOREIGN PATENT DOCUMENTS

138457 10/1979 German Democratic Rep.

OTHER PUBLICATIONS

"Single Chip Encrypts Data at 14 Mb/s" by MacMillan Electronics, vol. 54 #12 6/16/81 pp. 161-165.

Primary Examiner—Salvatore Cangialosi

Assistant Examiner—Aaron J. Lewis

Attorney, Agent, or Firm—Edward W. Callan

[57] ABSTRACT

In the scrambling system, an analog audio signal is converted into a digital signal to provide a sequence of digital signal samples corresponding to the analog audio signal. Each digital signal sample is compressed to provide compressed signal samples having a sign bit, three exponent bits and seven mantissa bits. Each bit of each compressed signal sample is exclusive-OR'd with a unique keystream to thereby scramble the audio signal. A Hamming code generator generates code bits for correcting singular errors in a combination of the sign bit, the exponent bits and the code bits; and a parity bit generator generates a parity bit for detecting double errors in a combination of the sign bit, the exponent bits and the code bits and for further detecting an error in the most significant mantissa bit and/or the parity bit. The bits from a plurality of successive compressed, error-encoded signal samples are interleaved and serialized in order to separate the bits from any single sample by at least a predetermined duration associated with an FM discriminator click. The serialized, interleaved, error-encoded, compressed signal samples are combined to provide two-bit digital words. The digital words are converted to digital PAM data signals which when converted to an analog signal by digital-to-analog conversion, provide a pulse-amplitude-modulated signal having a level related to the binary value of the digital words. The digital PAM data signals are converted to an analog signal to provide the pulse-amplitude-modulated signal. The descrambler system descrambles the scrambled audio signal by a process that is the converse of the scrambling process. Singular errors in a scrambled signal sample are detected and corrected by a Hamming error corrector. Double errors in a scrambled signal sample are detected by a parity bit check and compensated for by repeating the last received error free signal sample.

24 Claims, 9 Drawing Figures

[54] SIGNAL ENCRYPTION AND DISTRIBUTION SYSTEM FOR CONTROLLING SCRAMBLING AND SELECTIVE REMOTE DESCRAMBLING OF TELEVISION SIGNALS

[75] Inventors: Elein S. Gilhousen, San Diego; Charles F. Newby, Jr., El Cajon; Karl E. Moerder, Poway, all of Calif.

[73] Assignee: M/A-COM Linkabit, Inc., San Diego, Calif.

[21] Appl. No.: 498,808

[22] Filed: May 27, 1983

[51] Int. Cl.⁴ H04N 7/167; H04L 9/00

[52] U.S. Cl. 358/122; 178/22.07; 178/22.1; 178/22.16

[58] Field of Search 358/122; 178/22.07; 178/22.1, 22.14, 22.16

[56] References Cited

U.S. PATENT DOCUMENTS

3,238,297	3/1966	Pawley et al.	178/22
3,668,307	6/1972	Face et al.	178/5.6
3,729,581	4/1973	Anderson	178/6.8
3,777,053	12/1973	Wittig et al.	178/5.1
3,798,359	3/1974	Feistel	178/22
3,803,491	4/1974	Osborn	325/53
3,886,302	5/1975	Kosco	178/5.1
3,894,176	7/1975	Mellon	178/5.1
3,899,633	8/1975	Sorenson et al.	178/5.1
3,916,091	10/1975	Kirk, Jr. et al.	178/5.1
3,919,462	11/1975	Hartung et al.	178/5.1
3,936,593	2/1976	Aaronson et al.	178/5.1
3,997,718	12/1976	Ricketts et al.	178/6.8
4,024,574	5/1977	Nieson	358/117
4,025,948	5/1977	Lochin	358/122
4,058,830	11/1977	Guinet et al.	358/86
4,068,264	1/1978	Pires	358/122
4,091,417	5/1978	Nieson	357/117
4,112,464	9/1978	Guif et al.	358/122
4,115,662	9/1978	Guinet et al.	179/15 BV
4,115,807	9/1978	Pires	358/122
4,160,120	7/1979	Barnes et al.	178/22
4,161,751	7/1979	Ost	358/114
4,163,254	7/1979	Block et al.	358/122
4,163,255	7/1979	Pires	358/122
4,172,213	10/1979	Barnes et al.	178/22
4,215,366	7/1980	Davidson	358/124
4,225,884	9/1980	Block et al.	358/122
4,250,524	2/1981	Tomizawa	358/122
4,253,114	2/1981	Tang et al.	358/114
4,292,650	9/1981	Hendrickson	358/123
4,302,771	11/1981	Gargini	358/86
4,304,990	12/1981	Atalla	235/379
4,316,055	2/1982	Feistel	178/22.06

4,322,745	3/1982	Saeki et al.	358/123
4,323,921	4/1982	Guillou	358/114
4,323,922	4/1982	den Toonder et al.	358/117
4,331,973	5/1982	Eskin et al.	358/84
4,331,974	5/1982	Cogswell et al.	358/86
4,336,553	6/1982	den Toonder et al.	358/120
4,338,628	7/1982	Payne et al.	358/120
4,354,201	10/1982	Sechet et al.	358/122
4,388,643	6/1983	Aminetazah	358/122
4,458,109	7/1984	Mueller-Schloer	178/22.16
4,461,032	7/1984	Skerlos	435/4
4,467,139	8/1984	Mollier	178/22.08
4,471,164	9/1984	Henry	178/22.11
4,484,027	11/1984	Lee et al.	358/122
4,531,011	7/1985	Bluestein et al.	178/22.08
4,531,020	7/1985	Wechselberger et al.	178/22.08
4,533,948	8/1985	McNamara et al.	358/122
4,533,949	8/1985	Fujimura et al.	358/122
4,535,355	8/1985	Arn et al.	358/122

Primary Examiner—Stephen C. Buczinski

Assistant Examiner—Linda J. Wallace

Attorney, Agent, or Firm—Edward W. Callan

[57] ABSTRACT

A system and method for scrambling and selectively descrambling television signals that are transmitted to subscribers' descramblers in a subscription television system. A working key signal is generated by processing an "initialization vector" signal in accordance with the DES algorithm upon the algorithm being keyed by either a common category key signal or some other key signal. A unique encryption keystream is generated by processing the initialization vector signal in accordance with the DES algorithm upon the algorithm being keyed by the working key signal. A television signal is scrambled in accordance with the unique encryption keystream to provide a scrambled television signal. A plurality of unique encrypted category key signals individually addressed to different selected subscribers' descramblers are generated by processing the initial common category key signal in accordance with the DES algorithm upon the algorithm being keyed by a plurality of different "unit key" signals unique to different selected descramblers. The scrambled television signal, the initialization vector signal, and the plurality of encrypted category key signals are broadcast to the descramblers. A corresponding tier of DES algorithms are employed at the descrambler to reproduce the encryption keystream; and the TV signal is descrambled in accordance therewith. Each descrambler has its unique unit key signal stored in a secure memory for use in reproducing the common category key signal when the descrambler is addressed by its unique encrypted category key signal.

26 Claims, 8 Drawing Figures

